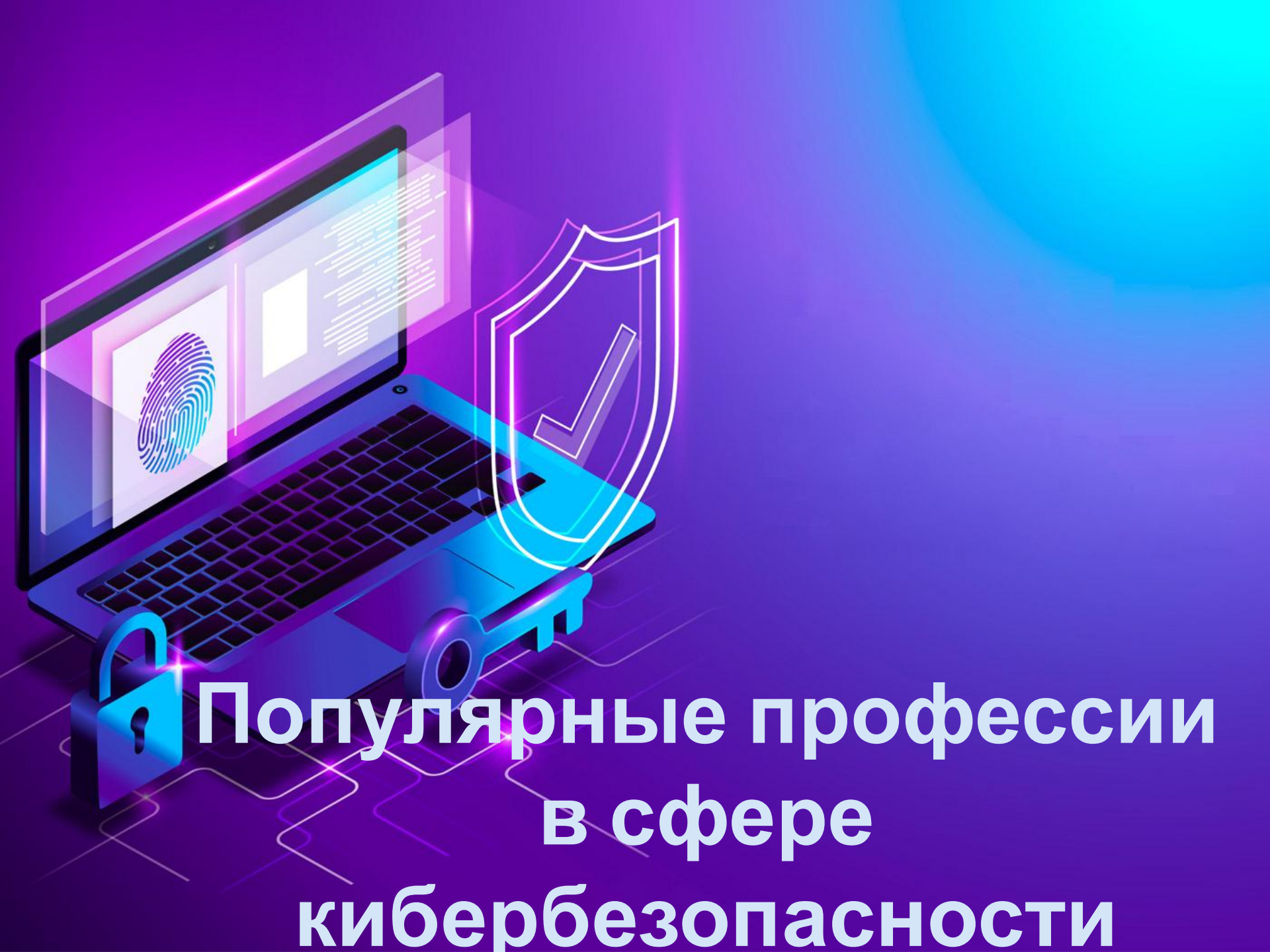

Популярные профессии в сфере кибербезопасности

Что делает специалист по кибербезопасности

Выявляет угрозы информационной безопасности и риски потери данных, вырабатывает и внедряет меры противодействия угрозам и решения для защиты от потери информации; обеспечивает сохранность и конфиденциальность данных; участвует в разработке и внедрении IT-решений.

Профессиональные уровни специалистов по кибербезопасности

- Junior – младший специалист
- Middle – средний специалист
- Senior – старший специалист

Какими знаниями должен обладать специалист Junior

Претендовать на данную позицию можно практически любому айтишнику после прохождения специализированных курсов. Так или иначе, специалист уровня Junior должен обладать как минимум следующими компетенциями:

- владение базовыми знаниями по сетям и операционным системам;
- понимание принципов статистической маршрутизации, адресации IP, знание ISO/OSI, TCP/IP;
- наличие хотя бы начального опыта администрирования Active Directory для настройки групповой политики и управления правами пользователей;
- опыт по настройке защиты на базе Windows и ведущих антивирусов;
- умение настроить базу данных: MySQL и Apache2, Rsyslog и Auditd, PostgreSQL и nginx.

Какими знаниями должен обладать специалист Middle

Для перехода на средний уровень требуется уже более серьезный багаж знаний и навыков, который включает:

- понимание принципов построения и работы сетей ISO/OSI, TCP/IP, принципов безопасности веб-приложений, компьютерной и сетевой безопасности;
- понимание принципов работы корпоративных антивирусов и систем обнаружения кибератак;
- владение операционными системами Windows и Linux на уровне администратора;
- опыт автоматизации на основе Bash, Perl, Python;
- умение выполнять анализ информационной защищенности.

Какими знаниями должен обладать специалист Senior

К старшему специалисту в области кибербезопасности предъявляются существенные квалификационные требования. Он должен обладать следующими знаниями и навыками:

- владение законодательной и нормативной базой в сфере информационной защиты;
- знание основных классификаций, методик и международных практик — NIST SP800-115, WASC, OSSTMM, OWASP;
- написание программ на скриптовых языках;
- навыки выявления киберугроз;
- уверенное владение профильным софтом: Cisco ASA, Imperva DAM, IBM Qradar, Maxpatrol, System Protection, Gigamon Networks Tuffin и т. д.;
- способность работы с системами узкого профиля: SCADA, SS7, ERP, Hardware;
- опыт в сборе улик и проведении расследований по результатам кибератак.

На какую работу можно устроиться

- Анти-фрод аналитик
- Пентестер
- Аналитик кода или специалист по реверс-инжинирингу
- Форензик
- Разработчик системы защиты информации (СЗИ)

Анти-фрод аналитик

Востребован в банковской сфере и финтех компаниях. Отвечает за безопасность онлайн-операций с финансами для физических лиц, например, в "онлайн-банке". Устанавливает и отслеживает лимиты на количество покупок по одной банковской карте, на максимальную сумму разовой покупки по одной карте или одним пользователем, количество банковских карт, используемых одним пользователем в определенный период времени. Ведет учет и анализирует историю покупок пользователей для выявления подозрительных операций.

Пентестер

Специалист, который тестирует систему, проверяет, насколько хорошо защищены данные. Выявляет слабые места, укрепляет защиту данных. Исследует целостность информационной системы. Пентестеров нанимают, обычно, крупные IT и финансовые компании, которые оперируют большими данными. Пентестерам необходимы глубокие знания ОС Windows\Linux, сетей, уязвимостей.

Аналитик кода илиспециалист по реверс-инжинирингу

В задачи специалиста входит детальный разбор программного кода с целью выявить уязвимости программы для кибератак. Специалист должен понимать общие принципы программирования, знать языки, как минимум C++, ASM, Python, знать виды уязвимостей OWASP Top 10, SANS Top-25. После анализа кода и выявления угроз специалист дает рекомендации по защите системы.

Форензик

Специалист, занимающийся расследованием киберпреступлений. Обычно представителей этой профессии нанимают для выполнения какой-то разовой проблемы. Чаще всего им предстоит иметь дело со взломанными серверами, СУБД, десктопами. Задача форензик-специалиста состоит в нахождении следов проникновения, восстановлении цепочки событий, выявлении нарушений. Он занимается сбором улик и разоблачением хакерских группировок, владеет популярными языками программирования и понимает, как киберпреступники обходят существующие системы защиты.

Разработчик системы защиты информации (СЗИ)

Специалист совмещает в себе знания и навыки разработчика со знанием средств защиты информации. Важны навыки программирования, знание языков CI\CD, облака AWS или MS Azure, фреймворков, антивирусов и DLP-систем. Разрабатывает в компаниях внутреннюю систему защиты информации и отслеживания кибератак.

ВУЗы по кибербезопасности: Где учат специалистов по информационной безопасности

Национальный исследовательский технологический университет «МИСиС»
Информатика и вычислительная техника (Институт информационных технологий и компьютерных наук)

Национальный исследовательский университет «МЭИ»
Безопасность компьютерных систем (Инженерно-экономический институт НИУ «МЭИ»)

Московский государственный университет пищевых производств
Информатика и вычислительная техника (Институт промышленной инженерии, информационных технологий и мехатроники)

Московский технический университет связи и информатики
Информатика и вычислительная техника (Заочный общетехнический факультет МТУСИ)

Московский государственный университет геодезии и картографии
Информационная безопасность (Московский государственный